

REMARKS

Applicant respectfully requests reconsideration and allowance in view of the foregoing amendments and the following remarks. Applicant notes that claim 1 has been amended and that claims 5-7 have been added. Thus, claims 1-7 are pending in the application.

Objection to Drawings:

In the Office Action, the sole drawing was object for having a "1/1" label at the top portion of the drawing. Applicant has submitted herewith a proposed drawing correction that deletes the "1/1" label.

Section 102 Rejections:

In the Office Action, claims 1, 2 and 4 were rejected under 35 U.S.C. 102(b) as being anticipated by Ehram (US Patent No. 4,386,234).

With regard to independent claim 1, Applicant notes that this claim has been amended to more particularly recite that during encryption of the digital data, a data bit word generated on the basis of random numbers is stored in a storage cell (10) before a data word is written therein such that the storage cell (10) is pre-initialized with random data. In contrast, Ehram generally describes a security device that automatically overwrites an old master cipher key with an arbitrary value when a new master cipher key is written into the storage device. Applicant notes, however, that after the new cipher key is written into memory, the key invalid latch is left set so that no data can be processed until after another valid key is installed by either a load key order (LKD) or decipher key order (DECK). Col. 36, lines 59-62; Col. 39, lines 39-46. If no data can be processed by the security device, Applicant respectfully submits that the process described in Ehram cannot be performed during encryption of digital data as recited in claim 1.

Furthermore, Ehram specifically states that the write master key (WMK) order described above "is performed infrequently and is done only under physically secure conditions." Col. 36, lines 65-66; Col. 9, lines 39-42 (indicating that the master key does not generally change for long period of time). In this context, the process described in Ehram only deals with new installations of master keys that are "used only by the cryptographic apparatus for internally deciphering enciphered keys which may be then be used as the working key in subsequent encipher/decipher operations." Col. 9, lines 56-60. Applicant, accordingly, respectfully submits that the process described in Ehram is only performed during installation of master keys, and is not performed during encryption of digital data as recited in claim 1. Embodiments of claim 1 provide significant advantages over Ehram by providing mechanisms that effectively prevents

crypto analysis by observation of current consumption during encryption of digital data. Therefore, because Ehram fails to teach or suggest claim 1, Applicant respectfully requests that the Section 102(b) rejections with respect to claim 1 and all claims dependent thereon be withdrawn.

Section 103 Rejections:

In the Office Action, claim 3 was rejected under 35 USC 103(a) as being unpatentable over Ehram in view of Yasuhiko (JP 01-298829). Applicant notes that the deficiencies of Ehram were discussed above with respect to claim 1. Applicant respectfully submits that the addition of Yasuhiko fails to alleviate these deficiencies. Therefore, Applicant respectfully requests that the Section 103(a) rejection with respect to claim 3 be withdrawn.

New Claims:

Applicant has also added new claims 5-7, which Applicant believes further defines over the cited art of record.

In view of the foregoing amendments and remarks, Applicant respectfully submits that claims 1-7 are in condition for allowance. Applicant, accordingly, respectfully requests that a notice of allowance be issued with respect to claims 1-7.

Please charge any fees which may be required, except the issue fee, or credit any overpayment to Deposit Account No. 14-1270.

Date: February 26, 2004

Respectfully submitted,

By



Kevin Simons, Reg. No. 45,110

(408) 474-9075

Philips Electronics North America

1109 McKay Drive; Mail Stop SJ41

San Jose, CA 95131 USA